GIBSON DUNN

Gibson, Dunn & Crutcher LLP

200 Park Avenue
New York, NY 10166-0193
Tel 212.351.4000
www.gibsondunn.com

Reed Brodsky
Direct: +1 212.351.5334
Fax: +1 212.351.6235
RBrodsky@gibsondunn.com

November 13, 2017

VIA ECF

The Honorable Kiyo A. Matsumoto
United States District Court Judge
United States District Court for the Eastern District of New York
225 Cadman Plaza East
Brooklyn, NY 11201

Re: *United States v. Greebel*, S1 15 Cr. 637 (KAM)

Dear Judge Matsumoto:

We respectfully submit this letter regarding government witness Jackson Su, whom the government called to the stand at trial this morning. As Your Honor knows, toward the end of his direct examination before the lunch break, Mr. Su admitted that he had accessed information from the Global Relay system after leaving Retrophin and MSMB in or about mid-December 2012. At a break outside of the presence of the jury, we raised the issue that Mr. Su's conduct may well have violated federal anti-hacking statutes.

Your Honor understandably called the CJA attorney on duty, John Burke, who then met alone with Mr. Su. Mr. Burke then reported back to the parties at approximately 3 p.m. today that, if asked about his access to the Global Relay system after he left in December 2012, Mr. Su would invoke his Fifth Amendment right not to incriminate himself. Your Honor then asked us to submit a brief by 8:00 p.m. this evening as to what effect this development should have on Mr. Su's testimony. For the reasons set forth below, we believe that Mr. Su should be required to invoke his Fifth Amendment rights in front of the jury, and that once that happens, the Court should give the jury an adverse-inference instruction and then consider whether and what portions of Mr. Su's direct testimony will need to be stricken.

I. Background – Su's Testimony in Court Today

On direct examination the government initially asked Mr. Su whether, "in [his] role as COO," he "institute[d] any policy or process for monitoring emails." Tr. __:11 (Nov. 13,

2017).[1] Mr. Su explained that since the company "didn't want anybody to do any insider trading," he "reached out to a third-party vendor called Global Relay and enlisted their services." *Id.* __:16-19. Mr. Su explained that Global Relay was "an archiving system" that tracked "any email that was sent or received from anyone" with a particular domain name. *Id.* __:21-24. Global Relay "automatically . . . grabbed emails and put them in an archive." During his time as COO, Mr. Su would, "from time to time," access the Global Relay archive remotely and maintain files both "in the office" and "at home." *Id.* __:19-20.

The government then established that Mr. Su left Retrophin in December 2012:

Q: When did you leave Retrophin?
A: A week before Christmas, so it would be some 20th time frame.
Q: December 20th, 2012?
A: Of 2012, yes.

Id. __:15-19. The government then asked Mr. Su to explain how he accessed Retrophin's private computer systems several months after leaving the company. Specifically, Mr. Su testified as follows:

Q: . . . Do you recall early on we talked about this email system.
A: Yes.
Q: And you said you believe that you printed certain documents and took them home with you?
A: Yes.
Q: After you left Retrophin on or about December 20th, did you keep those documents that you took home with you?
A: Yes.
Q: ***And did you continue to access that online email archive system?***
A: ***Infrequently but yes. (Archive.)***
Q: ***For how long did you continue to access that email archive system?***
A: ***Through March 2013.***
Q: ***And did you safe [sic] or print some of the emails you saw?***
A: ***Yes.***

Id. __:13-__:3 (emphasis added).

[1] Note that at the time of this writing, we have not received the final transcript for today's session so we are working off the rough Live Note version.

The government then proceeded to offer GX 685, to which we objected. We note that the government does not dispute that GX 685 was "printed by admin@msmbcapital.com on 2013-03-06." Nor does the government take issue with our contention that this document was obtained by Mr. Su through the Global Relay system after he left in December 2012.

The Court then conducted a lengthy sidebar, which gave rise to the issue at hand.

II. Given Su's Testimony, We Are Entitled to Cross-Examine Him about Whether He Violated Certain Federal Anti-Hacking Statutes

As an initial matter, it is undisputed that we have the right to cross-examine Mr. Su regarding specific acts that are probative of truthfulness and credibility. *See, e.g.*, Fed. R. Evid. 608(b). Clearly, whether Mr. Su accessed materials through unlawful hacking in violation of federal law is the textbook definition of a question that pertains to credibility and truthfulness. It cannot, of course, be disputed that evidence of Mr. Su's fraudulent, impermissible access of private computer systems and his deceptive access to Global Relay go directly to the heart of his credibility. *See id.*; *see, e.g.*, *Gordon v. United States*, 383 F.2d 936, 940 (D.C. Cir. 1967) ("In common human experience acts of deceit, fraud, cheating, or stealing, for example, are universally regarded as conduct which reflects adversely on a man's honesty and integrity."). Indeed, as noted below, one of the leading statutes that Mr. Su may have violated, Title 18, United States Code, Section 1030, has the word "Fraud" in the actual title of the statute. 18 U.S.C. § 1030.

Moreover, any failures by Mr. Su to disclose his conduct, and any prior misstatements or misrepresentations to federal authorities relating to his access and use of Global Relay, are also highly probative of his veracity. Further, any overlooking of Mr. Su's hacking conduct is also relevant and probative of Mr. Su's bias and disposition to assist the prosecution in recounting his recollections.

III. Su's Hacking May Well Have Violated Federal Law

The Computer Fraud and Abuse Act ("CFAA"), Title 18, United States Code, Section 1030, criminalizes hacking when a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." *Id*. § 1030(a)(2)(C). Mr. Su's conduct here—hacking into Global Relay—falls well within the bounds of the CFAA's prohibitions. Indeed, "Congress enacted the CFAA in 1984 to address 'computer crime,' which was then principally understood as 'hacking' or trespassing into computer systems or data." *U.S. v. Valle*, 807 F.3d 508, 525 (2d Cir. 2015). In fact, Mr. Su's behavior here bears striking similarity to scenarios contemplated by Congress. *Id*. ("The [House Committee Report] to the original bill described one instance of

'computer crime' in which an individual 'stole confidential software by tapping into the computer system of a previous employer from [the] defendant's remote terminal.'").

Mr. Su's behavior arguably violates other criminal statutes as well. The Stored Communications Act ("SCA"), Title 18, United States Code, Section 2701, makes it unlawful to "intentionally access[] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system." The Second Circuit has interpreted that section to not only prohibit third party disclosure, but also to "protect[] the privacy interests of users in many aspects of their stored communications from intrusion by unauthorized third parties." *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 217–18 (2d Cir. 2016), *cert. granted sub nom. United States v. Microsoft Corp.*, No. 17-2, 2017 WL 2869958 (U.S. Oct. 16, 2017); *see also* Wiretap Act, 18 U.S.C. § 2511(1)(a); Identity Theft, 18 U.S.C. § 1028. Mr. Su's conduct may also have violated state criminal statutes in New York and those states from where Mr. Su accessed the Global Relay system after leaving in or about December 2012.

IV. Through Counsel, Su Has Now Indicated that When Confronted, He Will Invoke His Fifth Amendment Rights

After hearing from both parties, the Court stated that it was "going to appoint counsel" since "I think he should have advice of counsel if he is going to talk about things that could implicate his Fifth Amendment right against self-incrimination." Tr. ___:20-23.

Mr. Burke then met with Mr. Su alone, and reported back to the Court and the parties – outside the presence of the jury – that Mr. Su would "be asserting his Fifth Amendment privilege" to questions relating to his access of Global Relay after he left in December 2012. Tr. __:19–20.

V. Su Should Have to Invoke His Fifth Amendment Rights in the Jury's Presence

To the extent that Mr. Su intends to invoke his Fifth Amendment right not to incriminate himself, he must do so in front of the jury. Where a government witness indicates he will refuse to testify pursuant to his Fifth Amendment right, a defendant "may ask questions on cross-examination that elicit the witness's assertion of his Fifth Amendment rights," and "the jury is entitled to an adverse inference instruction explaining what it may, but is not required to, infer from the witness's refusal to answer certain questions." *See United States v. Colasuonno*, No. 05 CR. 1110 (AKH), 2006 WL 3025880, at *3 (S.D.N.Y. Oct. 24, 2006); *see also Whitley v. Ercole*, 509 F. Supp. 2d 410, 414 n.1 (S.D.N.Y. 2007) (same).

VI. Once Su Invokes His Fifth Amendment Rights, the Court May Need to Strike His Testimony in Full

The Sixth Amendment's Confrontation Clause guarantees a criminal defendant's right to "test the truth of [government] witnesses' testimony through cross examination." *United States v. Cardillo*, 316 F.2d 606, 610 (2d Cir. 1963). If a district court allows a government witness to refuse to answer cross-examination questions pursuant to his Fifth Amendment privilege against self-incrimination and thereby "precludes inquiry into the details of his direct testimony, there may be a substantial danger of prejudice because the defense is deprived of the right to test the truth of his direct testimony and, therefore, that witness's testimony should be stricken in whole or in part." *Id.* This constitutes reversible error. *Id.*; *see also Klein v. Harris*, 667 F.2d 274, 289 (2d Cir. 1981); *cf. United States v. Crews*, 856 F.3d 91, 100 (D.C. Cir. 2017) (applying *Cardillo* to affirm district court's striking of direct testimony after witness invoked privilege).

In *Cardillo*, the Second Circuit distinguished between "cases in which the assertion of the privilege merely precludes inquiry into collateral matters which bear only on the credibility of the witness and those cases in which the assertion of the privilege prevents inquiry into matters about which the witness testified on direct examination." *Cardillo*, 316 F.2d at 611. As to one witness who invoked his privilege with respect to cross-examination relating to other crimes, the court held such testimony "merely collateral" because it related solely to his prior "substantial criminal record." *Id.* By contrast, as to another witness who had testified on direct as to facts at issue in the case and then invoked his privilege during cross-examination on those topics, the Second Circuit reversed the trial judge's failure to strike the witness's direct testimony. *Id.* at 612. The Second Circuit reasoned, "Disclosure of a direct lie relating to the events testified to might have had far more influence on the court's ultimate decision than testimony merely establishing the unsavory character of the witness by admissions of prior crimes." *Id.* at 612–13.

The Second Circuit's framework for analyzing whether and how much prior testimony to strike in the face of a witness who invokes his Fifth Amendment privilege is widely used in federal courts. *See Crews*, 856 F.3d at 99 (collecting cases). In *Crews*, the D.C. Circuit explained the *Cardillo* framework at length. With respect to whether refusing to answer cross-examination questions regarding a witness's credibility may require striking direct testimony on the same point, the court explained that *Cardillo* "does not treat all questions concerning credibility as 'collateral,' nor does it suggest that the related testimony of a witness who refuses to answer questions going only to credibility need never be stricken. That would make no sense; witness credibility is sometimes the linchpin of an entire defense." *Crews*, 856 F.3d at 100.

Here, on direct examination by the government, Mr. Su has already testified to facts giving rise to potential criminal liability under federal hacking laws. *See* Part I. His court-appointed attorney informed the parties that Mr. Su will invoke his Fifth Amendment right by refusing to answer cross-examination questions about his unauthorized access of Retrophin's private computer systems after leaving Retrophin in December 2012 and "[t]hrough March 2013." Tr. __:__ (Nov. 13, 2017). If the Court allows him to refuse to testify, we will be prevented from cross-examining him on an important aspect of his direct testimony, in violation of Mr. Greebel's Sixth Amendment right to confront witnesses against him.

Accordingly, we respectfully request that the Court require Mr. Su to invoke his Fifth Amendment right in front of the jury, give the jury an adverse-inference instruction if he refuses to testify, and consider whether to strike some or all of his direct testimony from the record.

Respectfully,

/s/ Reed Brodsky

Reed Brodsky

cc: Alixandra E. Smith, Esq.
David C. Pitluck, Esq.
David K. Kessler, Esq.